CLAIMS

What is claimed is:

1. A method, comprising:

downloading a boot image onto a mobile communication device;

generating a device-bound certificate ("DBC"), said DBC comprising an authentication code generated using a hashed message authentication code algorithm and a key specific to said device; and

storing the DBC in the boot image.

2. The method of claim 1, wherein generating a DBC comprises using an Open Multimedia Applications Platform ("OMAP") read-only memory ("ROM") code.

3. The method of claim 1, wherein generating a DBC comprises executing a protected application in a secure execution environment.

4. The method of claim 1, wherein generating a DBC comprises storing device-specific information in said DBC.

5. The method of claim 4, further comprising verifying authenticity, integrity and unique association of said device-specific information to the mobile communication device during a booting process.

6. The method of claim 5, further comprising interrupting the booting process if said verification is unsuccessful.

7. The method of claim 4, wherein storing device-specific information comprises storing an International Mobile Equipment Identifier number.

8. The method of claim 1, further comprising encrypting the DBC.

9. The method of claim 1, further comprising verifying authenticity and integrity of the authentication code.

10. The method of claim 9, wherein verifying the authenticity and integrity of the authentication code comprises preventing completion of a booting process if said verification is unsuccessful.

11. A mobile communication device, comprising:

a flash memory; and

an OMAP processor comprising a ROM code and coupled to the flash memory, said ROM code adapted to:

generate a device-bound certificate ("DBC");

encrypt the DBC; and

store the DBC on a boot image;

wherein said DBC comprises an authentication code generated using a hashed message authentication code algorithm and a key specific to said device.

12. The device of claim 11, wherein the ROM code verifies authenticity and integrity of the authentication code.

13. The device of claim 12, wherein the ROM code prevents completion of a booting process if said verification is unsuccessful.

14. The device of claim 11, wherein the DBC comprises device-specific information.

15. The device of claim 14, wherein the ROM code further verifies authenticity, integrity and unique association of said device-specific information to the mobile communication device during a booting process.

16. The device of claim 14 further comprising a protected application, wherein said protected application verifies authenticity, integrity and unique association of said device-specific information to the mobile communication device during a booting process.

17. The device of claim 15, wherein the ROM code interrupts the booting process if said verification is unsuccessful.

18. The device of claim 14, wherein the device-specific information comprises an International Mobile Equipment Identifier number.

19. The device of claim 14, wherein the device-specific information comprises at least one SIMlock file.

20. A computer readable medium containing instructions that are executable by a computer system, and when executed the instructions implement a method comprising:

generating a device-bound certificate ("DBC"), said DBC comprising an authentication code generated using a hashed message authentication code algorithm and a key specific to said medium; and

storing the DBC on the boot image.

21. The computer readable medium of claim 20, wherein generating a DBC comprises using an OMAP ROM code.

22. The computer readable medium of claim 20, wherein generating a DBC comprises executing a protected application in a secure execution environment.

23. The computer readable medium of claim 20, wherein generating a DBC comprises storing device-specific information in said DBC.

24. The computer readable medium of claim 23, further comprising verifying authenticity and integrity of said device-specific information during a booting process.

25. The computer readable medium of claim 20, wherein the method further comprises verifying authenticity and integrity of the authentication code during a booting process.

26. A mobile communication device, comprising:

a flash memory;

a boot image bound to said flash memory using an authentication code generated by way of a hashed message authentication code algorithm and a key specific to said device; and

an OMAP processor comprising a ROM code and coupled to the flash memory, said ROM code adapted to verify the authenticity and integrity of said authentication code.

27. The device of claim 26, wherein the ROM code prevents completion of a booting process if said verification is unsuccessful.

28. The device of claim 26 further comprising a protected application, wherein said protected application prevents completion of a booting process if said verification is unsuccessful.

29. The device of claim 26, wherein the boot image comprises device-specific information.

30. The device of claim 29, wherein the ROM code verifies authenticity and integrity of said device-specific information and prevents completion of a booting process if said verification is unsuccessful.